AMSEL-IE-TI No. BR 00/001
April 2000

Security Certification -

Telling it like it is!

Prepared for the

ISEC Critical Skills Lecture Series

John V. Kimbell
USAISEC CSE for
Security Certification
April 2000

Distribution A. Approved for public release.

Security Certification

- **Purpose**

The purpose of this class is to acquaint the audience with the security certification process.

- **Scope**

This class is intended to be an explanatory overview of what that process entails - who does what, and what do they do?

Certification is NOT rocket science!

Rocket science is trivial!!!

Why Do We Certify and Accredit Systems?

"Before operation, each AIS will be certified and accredited under a set of security requirements and safeguards approved by the DAA."

AR 380-19, para 2-3a(9)

Accreditation:

"Accreditation is the official managerial
authorization to operate an AIS or netwo
is based, in part, on the formal certificati
the degree to which a system meets a pre
set of security requirements."

AR 380-19, para 3.1 c

Certification:

"Certification is a technical evaluation of
effectiveness of AIS security features and
supports the accreditation decision. Certi
verifies that the AIS security functions ar
correctly implemented and sufficient to s
the mode of operation and the security po
for the system in an intended operational
environment."

AR380-19, para 3.4 a

The Certification Authority (CA):

- Acts as a trusted agent of the Designated Approving Authority (DAA).
- Provides support to the DAA by conducting a comprehensive evaluation of both the technical and non-technical security features of the system under evaluation.
- Recommends to the DAA whether or not to accredit the system after the certification process is completed.

The Certification Authority (CA):

- The CA must be independent from the organization responsible for the system development or operation. (Decreases the potential for conflicts of interest and allows for an impartial evaluation.)

The Four Phases of the DITSCAP:

Phase 1: Definition

Phase 2: Verification

Phase 3: Validation

Phase 4: Post Accreditation

Certification Levels:

Level 1: Minimum Security Checklist
Requires completion of the minimum security checklist
The system user or an independent certifier may compl
checklist.

Level 2: Minimum Analysis
Requires completion of the minimum security checklist
and independent certification analysis as defined in th
Verification and Validation phases.

Certification Levels (cont'd):

Level 3: Detailed Analysis
Requires completion of the minimum security checklist
and more in-depth, independent analysis as defined in the
Verification and Validation phases.

Level 4: Extensive Analysis
Requires completion of the minimum security checklist and the most extensive independent analysis as defined in the
Verification and Validation phases.

Characteristic	System Selection Alternative Values	Assigned Weight =
Interfacing Mode	Benign (w=0), Passive (w=2), Active (w=6)	
Processing Mode	Dedicated (w=1), System High (w=2), Compartmented Level (w=5), Multi-level (w=8)	
Attribution Mode	None (w=0), Rudimentary (w=1), Basic (w=3), Comprehensive (w=6)	
Mission-Reliance Factor	None (w=0), Cursory (w=1), Partial (w=3), Total (w=7)	
Accessibility Factor	Reasonable (w=1), Soon (w=2), ASAP (w=4), Immediate (w=7)	
Accuracy Factor	Not-applicable (w=0), Approximate (w=3), Exact (w=6)	
Information Categories	Unclassified (w=1), Sensitive (w=2), Collateral Classified (w= 6), Compartmented/Special Access Classified (w=9)	
Total of all weights.		

Certification Level	Weight
Level l	If the total of the weighing factors in Table 3-1 are < 16.
Level 2	If the total of the weighing factors in Table 3-1 are 12 - 32.
Level 3	If the total of the weighing factors in Table 3-1 are 24 - 44.
Level 4	If the total of the weighing factors in Table 3-1 are 38 - 50.

Areas of possible contention:

1 - 4	5 - 8	9 - 12	13 - 16	17 - 20	21 - 24	25 - 28	29 - 32	33 - 36	37 - 40	41 - 44	45 - 48	49-50
LEVEL I												
			LEVEL II									
						LEVEL III						
										LEVEL IV		

Requirements Traceability Matrix (RTM).

Analyze the directives and security requisites to determine the system security requirements. Take a section of a directive and parse it into a basic security requirement statement. The security requirements may then be entered into an RTM to support the remainder of the C&A effort.

Source Document	Paragraph	SSRS Reference	Certification Procedure Reference	Evaluation Method	Met	Not Met
AR 380-19	2-3a(2)	2.2.1.1	4.2.1.3.1	I	X	
AR 380-19	2-14i	2.2.2.5	4.2.2.3.9	A	X	
AR 380-19	2-14h	2.2.2.13	4.2.2.3.21	D	X	
AR 380-19	2-24e	2.2.1.9	4.2.1.3.13	T		X

2.3a(2): The identity of each user authorized access to the AIS will be established positively before authorizing access. If a password system is used to authenticate access, it shall adhere to the minimum requirements in Paragraph 2-15.

2.14(i): All passwords should be generated by random generator software and must not be obtained from commonly used words or phrases.

2.14(h): Passwords will be inhibited, overprinted, or otherwise protected from unauthorized observation on terminals and video displays.

2.24(e): Systems that process classified or unclassified-sensitive information will limit the number of user log-on attempts to three before access by that user is inhibited. Users will not be reinstated until the ISSO or his or her designee has verified the reason for failed log-ons.

The Security Engineer and Certification

- The security engineer and the CA maintain a close relationship during the certification and accreditation process.
- The security engineer must be made aware of any extremely high risks as soon as they are identified.

Documents Received from the Security Engineer:

1. System Design Plan (SDP)
2. Threat Description
3. Security Policy (includes System, Network, & Physical policies)
4. Configuration Management Plan (CMP)
5. Certification Plan (with CA)
6. Continuity of Operations Plan (COOP)
7. System Security Requirements Specification (SSRS)
8. Security Training & Awareness Plan
9. Trusted Facilities Manual (TFM)
10. Security Features Users Guide (SFUG)

DOCUMENTS PRODUCED BY THE USAISEC CERTIFICATION TEAM

System Test and Evaluation (ST&E) Plan

- A detailed description of the testing of security features to be performed during development in a lab environment in support of certification.

- Describes the specific requirement (referenced to the SSRS), states the purpose of the test and delineates the criteria for success.

1.0 Security Policy

1.1 RTM# Source: (AR 380-19, Orange Book, etc.)

1.1.1 Requirement to be tested:

1.1.2 Test Objective (Purpose):

1.1.3 Test Method (Inspection, Test, or Analysis): (Inspection, test, evaluate, demonstration)

1.1.4 Test Scenario (Test Setup):

1.1.5 Test Procedures

1.1.6 Expected Results:

1.1.7 Actual Results:

1.1.8 Overall Results/Conclusions: Met_____ Not Met_____

1.1.9 Comments:

1.1.10 Date Tested_____ Tested By_____

Risk Assessment Report (RAR)

Includes an examination of threats, vulnerabilities and the resulting risks.

For each risk that is unacceptably high, the RAR describes the security weakness and explains why it constitutes a vulnerability.

Fixes (enhanced or additional countermeasures) are suggested, along with an explanation of how they would reduce vulnerabilities and thus reduce the risk. “Initial risk” (as is) and “residual risk” (with the additional countermeasures) are estimated.

Probability of Successful Exploitation of a Vulnerability	Degree of Harm that Would Occur to the System or Data Due to Successful Exploitation	Risk Level
HIGH	HIGH	EXTREMELY HIGH
HIGH	MODERATE	HIGH
HIGH	LOW	MODERATE
MODERATE	HIGH	HIGH
MODERATE	MODERATE	MODERATE
MODERATE	LOW	LOW
LOW	HIGH	MODERATE
LOW	MODERATE	LOW
LOW	LOW	EXTREMELY LOW

3. Certification Evaluation Report (CER)

- Contains the “raw” results of the certification testing (ST&E) and forms the foundation for certification. It presents the overall security test plans and detailed procedures, with test results and comments from the testers.

- The number of attachments depends on the complexity of the system. For instance, one might want to organize them functionally and have one attachment for routers, one for terminal servers, one for print servers, one for e-mail servers, etc. Or one might want to organize them by equipment, and have one for Windows NT servers, one for Windows 95 platforms, one for CISCO devices, etc.

4. Certification Statement

The Certification Statement is the Certification Agent's report to the DAA on the results of the certification testing. It includes a recommendation to either accredit the system, or not. It may recommend an Interim Approval to Operate (IATO) for up to 6 months while high failures are being fixed.

It is prepared by the Certifying Agent.

Full Accreditation
The system is approved to operate in the intended environment as stated in the SSAA.

Interim Approval to Operate (IATO)
The system does not meet the requirements as stated in the SSAA, but mission criticality mandates the system become operational. The IATO is a temporary approval that may be issued for no more than a 1-year period. Use of the IATO requires a return to phase 1 to negotiate accepted solutions, schedule, necessary security activities, and milestones.

Before the IATO may be issued, phase 2 and 3 activities must be completed and appropriately documented. This ensures repeatability in the process.

Disapprove Accreditation
The system does not meet the requirements stated in the SSAA, accepted risk is too great and mission criticality does not mandate the immediate operational need. This type of accreditation requires a return to phase 1 to negotiate accepted solutions, necessary security activities, and milestones. The system must complete phases 2 and 3. This ensures repeatability in the process.

3.6 Reaccreditation

a. All AIS accredited under this regulation will be reaccredited within 3 months following any event below:

(1) Addition or replacement of a major component or a significant part of a major system.

(2) A change in classification level of information processed.

(3) A change in security mode of operation.

(4) A significant change to the operating syste
executive software.

(5) A breach of security, violation of system
integrity, or any unusual situation that appear
invalidate the accreditation.

(6) A significant change to the physical structure housing the AIS that could affect the physical security described in the accreditation.

(7) The passage of 3 years since the effective date of the existing accreditation.

(8) A significant change to the threat that could impact Army systems.

(9) A significant change to the availability of safeguards.

(10) A significant change to the user population.

b. Reaccreditation will include the same steps accomplished for the original accreditation; however, those portions of the documentation that are still valid need not be updated.

ANY QUESTIONS?